Terms used **shared library"; tamper resistant processor** Found **5** of **192,172**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 5 of 5

Relevance scale

1 Fast Secure Processor for Inhibiting Software Piracy and Tampering
Jun Yang, Youtao Zhang, Lan Gao
December 2003 **Proceedings of the 36th annual IEEE/ACM International Symposium on Microarchitecture**
Publisher: IEEE Computer Society
Full text available: pdf(258.88 KB) Additional Information: full citation, abstract, citings, index terms

Due to the widespread software piracy and virus attacks,significant efforts have been made to improve security forcomputer systems. For stand-alone computers, a key observationis that other than the processor, any component isvulnerable to security attacks. Recently, an execution onlymemory (XOM) architecture has been proposed to supportcopy and tamper resistant software [18, 17, 13]. In this design,the program and data are stored in encrypted formatoutside the CPU boundary. The decryption is ca ...

2 Virtual machine monitors: Implementing an untrusted operating system on trusted hardware
David Lie, Chandramohan A. Thekkath, Mark Horowitz
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Publisher: ACM Press
Full text available: pdf(280.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~---~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~---~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted.Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

3 Virtual machine monitors: Terra: a virtual machine-based platform for trusted computing
Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Publisher: ACM Press
Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a flexible architecture for trusted computing, called Terra, that allows

applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

4 Workshop on architectural support for security and anti-virus (WASSA): ChipLock: support for secure microarchitectures

Taeho Kgil, Laura Falk, Trevor Mudge

March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1

Publisher: ACM Press

Full text available: pdf(256.52 KB) Additional Information: full citation, abstract, references, index terms

The increasing need for security has caused system designers to consider placing some security support directly at the hardware level. In fact, this is starting to emerge as an important consideration in processor design, because the performance overhead of supporting security in hardware is usually significantly lower than a complete software solution. In this paper, we investigate integrating some security support into hardware. We show that security support can be added at some acceptable cos ...

5 Mondrix: memory isolation for linux using mondriaan memory protection

Emmett Witchel, Junghwan Rhee, Krste Asanović

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(332.09 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the design and an evaluation of Mondrix, a version of the Linux kernel with Mondriaan Memory Protection (MMP). MMP is a combination of hardware and software that provides efficient fine-grained memory protection between multiple protection domains sharing a linear address space. Mondrix uses MMP to enforce isolation between kernel modules which helps detect bugs, limits their damage, and improves kernel robustness and maintainability. During development, MMP exposed two kerne ...

Keywords: fine-grained memory protection

Results 1 - 5 of 5

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4561	shared with librar$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:03
L2	202	l1 same task	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:04
L3	7	l2 same (key or cipher)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:06
L4	5	l3 and (processor or microprocessor)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:16
L5	19	l2 same (processor or microprocessor)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:29
L6	19	l1 with authenticat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:38
L7	71	717/164.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L8	152	717/163.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L9	0	717/1623.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46

EAST Search History

L10	380	717/162.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L11	54	l1 and (l7 or l8 or l9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:47